이것만은 알아야 할 네트워크 보안 이야기

Part 2. 방화벽 - 2 (차세대방화벽, 웹 방화벽의 등장)

글. 이선응 아이크래프트 수석

앞에서 방화벽의 역할 및 보안정책에 대해 알아보았다. 이번 호에서는 기존 방화벽의 문제를 해결하기 위해 등장한 차세대방화벽 및 홈페이지 해킹 등 웹 서비스의 방어를 위해 등장한 웹 방화벽에 대해 알아보겠다.

우선 차세대방화벽을 설명하기 전에 방화벽의 기술발전 역사를 알아보도록 하자. 본격적인 방화벽이 나오기 전에는 통신을 전송하기 위한 통신장비인 라우터의 필터 기능에서부터 트래픽 제어 기능이 사용되었다. 우리가 데이터를 전송한다는 것은 최대 1,500byte의 크기로 잘게 쪼개진 데이터 묶음으로 만들어진 패킷(packet)을 보내고 받는 것을 말한다. 이 패킷의 헤더에는 출발지, 목적지 IP 주소와 서비스 포트가 기록되어 있다. 이 패킷 헤더 정보를 확인해서 라우터에 설정된 필터 정보를 참조하여 들어온 패킷을 허용하거나 차단하는 방식으로 동작한다.

이런 필터가 증가하게 되면, 라우터의 부하가 증가하게 되어 패킷 전송이라는 본래 기능에 문제가 생기게 되고, 고정된 포트를 사용하지 않고 접속할 때마다 서비스 포트가 변경되는 RPC, FTP 같은 서비스의 경우에는 인식이 불가능한 문제점이 발생하면서 트래픽 제어를 위한 전용 장비의 필요성이 제기되었다.
1994년 체크포인트(Checkpoint)라는 회사에서 이러한 문제점을 해결한 1세대 방화벽이 개발되었다. 개발된 방화벽의 가장 큰 특징은 스테이트풀 인스펙션(Stateful Inspection) 기능이 추가된 것이다. 단순히 들어 오는 패킷을 필터링하는 것이 아니라, 클라이언트와 서버 간 통신 상태를 모니터링하여 연결 테이블을 만들고 관리하면서 좀 더 세밀한 트래픽 제어가 가능해진 것이다.

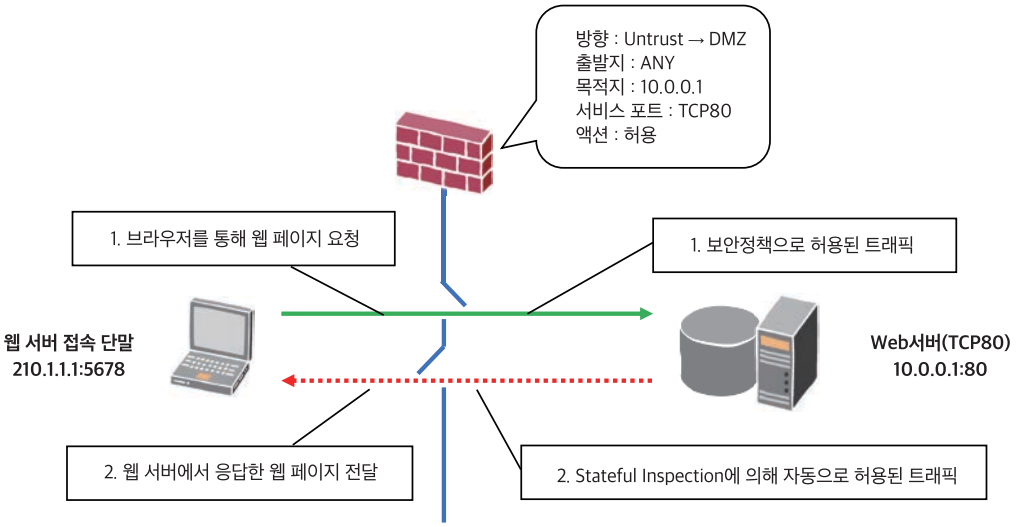

그림 1. 스테이트풀 인스펙션 (Stateful Inspection) 설명

[그림 1]을 보면 왼쪽의 단말 장비에서 오른쪽의 웹 서버로 접속을 시도한다고 가정해 보자. 방화벽에는 인터넷에서 DMZ 구역으로 들어오는 패킷에 대해 출발지는 ANY, 목적지는 10.0.0.1, 서비스 포트는 TCP 80 포트에 대해 허용하는 보안정책이 설정되어 있다.

접속 단말에서 서버로 웹 페이지를 요청하는 트래픽이 방화벽에 도착하면, 방화벽은 해당 요청에 대해 보안정책을 확인하여 해당 패킷을 오른쪽 웹 서버로 전달한다. 서버는 단말의 요청에 응답하기 위해 웹 페이지를 접속 단말을 목적지로 하는 패킷으로 생성하여 전송한다. 이 응답 패킷이 방화벽에 전달되면 방화벽은 다시 보안정책을 참고하여 패킷을 허용할 건지 차단할 건지 결정할 것을 예상할 수 있다.

이 단계에서 스테이트풀 인스펙션의 장점이 발휘된다. [그림 1] 방화벽 정책은 외부에서 DMZ 구역으로 갈 수 있는 보안정책이 있지만 반대 방향인 즉, DMZ 구역에서 외부로 나가게 허용하는 보안정책은 없다. 방화벽은 기본적으로 보안정책에 적용되지 않는 모든 패킷은 차단하게 되어있다. 즉, 서버에서 단말로 가는 응답 패킷은 차단될 것으로 예상할 수 있으나, 스테이트풀 인스펙션 기능이 동작하기 때문에 서버에서 보낸 페이지는 방화벽을 정상적으로 통과한다. 즉 방화벽이 만들어서 관리하는 세션 테이블(Session Table)을 참조하여 들어오는 응답 패킷의 출발지, 목적지 IP 및 Port와 일치하는 세션 리스트가 있는지 확인되면, 해당 패킷은 응답 패킷으로 판단하여 보안정책이 없더라도 해당 패킷을 클라이언트로 전달하는 것이다. 방화벽은 데이터를 요청하는 트래픽이 들어오면 서버로 전달하면서 동시에 세션 테이블을 만들어서, 서버와 클라이언트 간의 통신 내역을 모니터링하고 제어하는 용도로 사용한다.

다음 [그림 2]는 방화벽에서 출력한 세션 테이블이다. In 항목에 나와 있는 것과 같이 출발지 IP 10.10.10.235에서 출발지 포트 50588을 사용하여 st0.511 인터페이스로 들어와서 목적지 IP 172.70.1.13, 목적지 포트 TCP 7001로, 패킷 수 6개, 456byte 크기의 패킷이 보안정책 'untrust-to-trust'에 적용되어 목적지로 전달되었다. 다음으로 Out에 표시된 바대로 들어올 때와 출발지, 목적지 정보가 반대로 바뀌어서 서버에서는 데이터를 요청하는 단말로 응답 패킷을 4개, 427byte만큼 전송한 내역을 확인할 수 있다.

```
Session ID: 596, Policy name: untrust-to-trust/5, Timeout: 2, Valid
  In: 10.10.10.235/50588 --> 172.70.1.13/7001;tcp, If: st0.511, Pkts: 6, Bytes: 465
  Out: 172.70.1.13/7001 --> 10.10.102.235/50588;tcp, If: vlan.0, Pkts: 4, Bytes: 427
```

그림 2. 방화벽 세션 테이블

다시 말하면 방화벽은 요청 패킷이 들어오면 서버로 전달하면서 서버에서 다시 클라이언트로 응답할 패킷 정보를 예상하여 미리 세션 테이블을 만들어 둔다. 실제 응답 패킷이 들어오면 먼저 만들어 둔 세션 테이블에서 정보가 일치하는 세션 정보가 있는지 확인하고, 보안정책이 없더라도 패킷을 단말로 전달하는 것이다. 이 기능을 이용하면, 관리자가 서버의 응답 패킷을 예상해서 보안정책을 미리 만들어 둘 필요 없이 방화벽이 자동으로 응답 패킷에 대한 보안정책을 생성했다가 연결이 종료되면 삭제하는 것처럼 작동한다.

이런 작동 방식은 회사 내부에 있는 단말이 인터넷을 사용할 때도 동일하게 적용된다. 즉 Trust에서 Untrust 방향으로, 출발지는 단말 IP 대역이고 목적지는 ANY이며, 서비스 포트는 TCP 80으로 허용하는 보안정책이 있으면, 사내의 단말이 인터넷의 웹 서버로 요청 패킷을 보낸 후, 외부에서 내부로 들어오는 응답 패킷은 별도의 보안정책이 없더라도 인터넷에서 사내의 단말까지 전달되는데 아무런 문제가 없다. 인터넷에서 내부로 들어올 수 있는 통로가 필요할

때만 잠깐 생성되었다가 필요가 없으면 바로 삭제되는 것처럼 동작한다.
즉, 라우터의 필터 기능과 같이 외부에서 내부로 들어올 응답 패킷을 위한 보안정책을 미리 만들어 둘 필요가 없어, 미리 만들어 둔 보안정책을 통해 발생 가능한 잠재적인 보안위협을 감소시킬 수 있는 점이 1세대 방화벽의 가장 큰 장점이다.

다음으로 2세대 방화벽은 보통 차세대(Next Generation) 방화벽이라 하며 통상 줄여서 NG 방화벽이라고 호칭한다. 1세대 방화벽과 가장 큰 차이점은 단말이 사용하는 응용 프로그램(Application)을 인식해서 선별적으로 차단이 가능하다는 점이다. 1세대 방화벽은 포트 넘버로만 트래픽을 구분할 수 있었기 때문에 TCP 80을 사용하는 모든 트래픽은 모두 차단하거나 허용할 수밖에 없었다. 예를 들면 인터넷사용은 허용하면서 메신저나 P2P 다운로드 트래픽은 차단하고 싶거나, 인터넷 중에서도 유튜브, 인스타그램 등만 선별적으로 차단하는 보안정책은 모두 같은 TCP 80 포트를 사용하기 때문에 불가능하였다.

우리가 사용하는 인터넷과 같은 통신은 참가하는 모든 단말이 동일한 규칙으로 신호를 주고받아야 하는데 이런 통신 규약을 프로토콜(Protocol)이라고 한다. 그중에 가장 대표적인 것이 ISO(국제표준화기구)에서는 제정한 OSI 7 레이어 참조 모델이 있다. [그림 3] OSI 프로토콜의 3번째 Network 계층이 IP 주소를 정의하는 곳이며, 4번째 Transport 계층이 TCP 혹은 UDP의 포트 넘버를 정의하는 단계이다. 즉 1세대 방화벽은 4계층까지만 모니터링이 가능한 장비이기 때문에 마지막 7번째 Application 계층인 응용 프로그램 단계는 모니터링이 불가능하다.

차세대방화벽은 Application 계층 데이터 모니터링이 가능하여 4계층에서 같은 서비스 포트를 사용하는 프로그램이더라도 서로 구분이 가능하다. 즉 포트 넘버가 아니고 카카오톡 같은 메신저, 토렌트 같은 P2P 파일 공유 트래픽을 구분할 수 있다. 그뿐만 아니라 카카오톡 트래픽 중에서도 단순한 채팅 트래픽과 파일을 공유하는 트래픽을 구분할 수 있으므로 채팅만 허용하고 파일 전송만 차단하는 선별적인 제어가 가능하다.

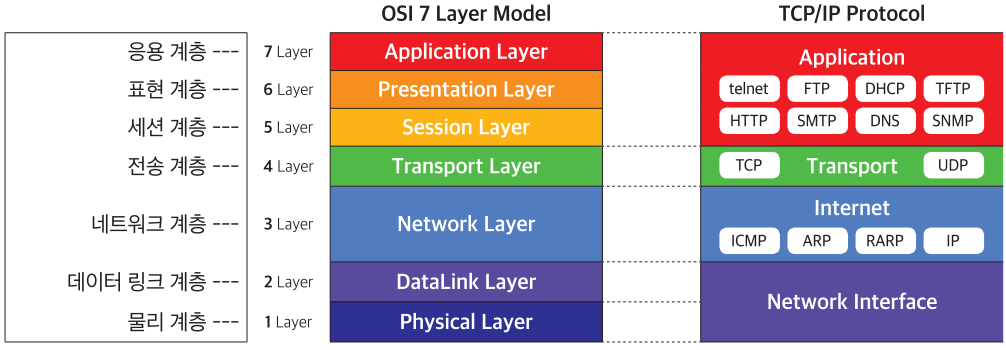

그림 3. OSI 7 레이어 및 TCP/IP 4 레이어 모델

그럼 차세대방화벽은 어떻게 애플리케이션을 구분할 수 있는지 알아보자. 다음 [그림 4]와 같이 패킷이 들어오면 일단 보안정책으로 포트 넘버를 먼저 확인한다. 그다음으로 패킷의 L7 레벨에 있는 데이터를 읽어서 방화벽이 가지고 있는 트래픽 패턴 정보와 동일한 패턴이 발견되는지 확인하여, 애플리케이션을 식별하고, 식별이 되지 않으면 다음으로 프로토콜 디코더라는 일종의 패킷 해석기를 이용하여 주고받는 내용의 특성을 분석하고 트래픽을 판별하는 방식을 이용한다. 이 단계에서도 판별이 되지 않으면 휴리스틱(Heuristic) 기법을 이용하여 정확하게 패턴이 일치하지 않더라도 통계적인 기법으로 유사도를 측정하여 80~90% 이상 패턴이 유사하면 특정 애플리케이션 트래픽으로 판별하는 방식으로 동작한다.

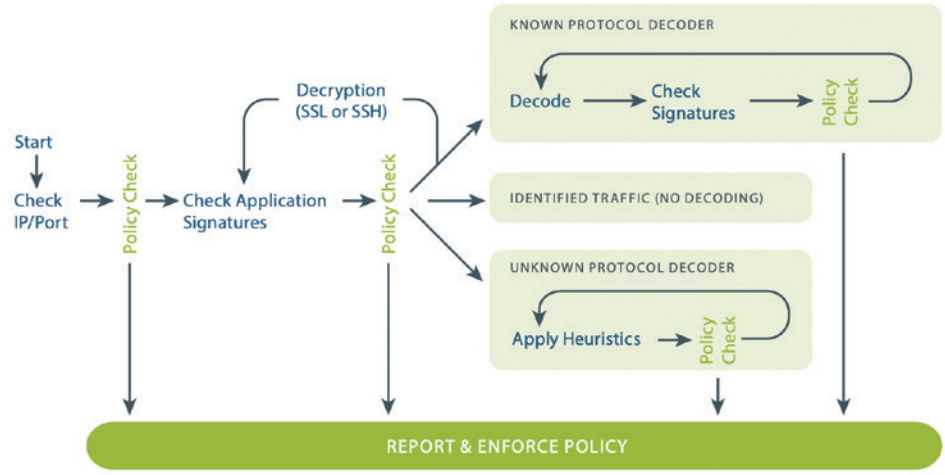

그림 4. Application 탐지 프로세스 / 출처 : 팔로알토 네트웍스

다음으로 현재 회사에서 많이 사용 중인 차세대방화벽에서 어떤 애플리케이션을 탐지하고 허용/차단할 수 있는지 알아보자. 최근 10년간 가장 트래픽을 많이 발생시키고 있는 프로그램 중의 하나는 단연코 P2P 파일 공유 프로그램들이다. 가장 대표적인 경우가 토렌트(torrent)이다. 웹하드와 같이 특정한 서버에 접속해서 파일을 다운로드받는 것이 아니라, 서버와 클라이언트가 구분되지 않고, 네트워크에 접속하는 각 개인이 보유 중인 파일을, 접속된 다른 사용자들에게 전송하는 서버 역할을 하고, 내가 없는 파일은 다른 사용자에게서 받아 오는 클라이언트 역할을 동시에 수행하는 프로그램이다.

이 프로그램의 특징은 일대일로 파일을 보내고 받는 것이 아니라, 내가 파일을 받을 때 하나의 파일을 여러 개로 쪼개서 여러 개의 단말에서 동시에 파일을 받을 수 있고, 반대로 파일을 보낼 때도 여러 개의 단말에 동시에 전송할 수 있는 점이다. 그래서 동일한 파일을 여러 단말이 많이 보유할수록 파일 전송속도가 빨라지는 특징이 있다. 문제는 대용량의 영상 파일을 주고받을 경우 많은 트래픽을 유발하기 때문에 집에서 사용하는 것은 문제가 없으나 회사 같은 조직 내에서 사용할 경우 네트워크 대역폭을 소모시켜서 업무에 지장을 줄 수 있는 점이다. 아래 [그림 5]는 방화벽에서 탐지할 수 있는 P2P 파일 공유 프로그램 목록이다.

NAME	CATEGORY	SUBCATEGORY	RISK	TECHNOLOGY
100bao	general-internet	file-sharing	5	peer-to-peer
aim				
└ aim-file-transfer	general-internet	file-sharing	4	peer-to-peer
allpeers	general-internet	file-sharing	5	peer-to-peer
ants-p2p	general-internet	file-sharing	5	peer-to-peer
applejuice	general-internet	file-sharing	5	peer-to-peer
ares	general-internet	file-sharing	5	peer-to-peer
azureus	general-internet	file-sharing	5	peer-to-peer
bittorrent	general-internet	file-sharing	5	peer-to-peer
direct-connect	general-internet	file-sharing	5	peer-to-peer
emule	general-internet	file-sharing	5	peer-to-peer
fasttrack	general-internet	file-sharing	5	peer-to-peer
fileguri	general-internet	file-sharing	5	peer-to-peer
fileswire	general-internet	file-sharing	5	peer-to-peer
flashget	general-internet	file-sharing	5	peer-to-peer
foxy	general-internet	file-sharing	5	peer-to-peer
generic-p2p	general-internet	file-sharing	5	peer-to-peer
globus	general-internet	file-sharing	2	peer-to-peer
gnunet	general-internet	file-sharing	5	peer-to-peer
gnutella	general-internet	file-sharing	5	peer-to-peer
goboogy	general-internet	file-sharing	5	peer-to-peer
google-talk				
└ gtalk-file-transfer	general-internet	file-sharing	5	peer-to-peer
imesh	general-internet	file-sharing	5	peer-to-peer
ip-messenger				
└ ip-messenger-file-transfer	general-internet	file-sharing	1	peer-to-peer
kazaa	general-internet	file-sharing	5	peer-to-peer
kugoo	general-internet	file-sharing	5	peer-to-peer
manolito	general-internet	file-sharing	5	peer-to-peer
ms-ocs-file-transfer	general-internet	file-sharing	2	peer-to-peer
msn				

그림 5. 패턴으로 등록된 P2P 파일 공유 프로그램 / 출처 : 팔로알토 네트웍스

목록에 보면 다양한 파일 공유 프로그램을 확인할 수 있고 분류 및 위험도, 기본통신방식 등이 나열되어 있다. 위험도는 벤더에서 임의로 지정한 등급으로 숫자가 높을수록 위험도가 높은 것으로 특정 등급을 묶어서 차단하거나 로그를 남기는 설정을 할 때 사용할 수 있다.
파일 공유 프로그램 이외에도 네이버 같은 포털 서비스, 다량의 트래픽을 유발하는 영상스트리밍 서비스인 유튜브(YouTube), 채팅과 파일 전송 기능이 있는 카카오톡, 최근 인기가 높아진 인스타그램과 같은 SNS 서비스 등도 식별이 가능하다. [그림 6]과 같이 네이버 트래픽에서도 블로그, 라인과 같은 메신저, 메일, 엔드라이브 같은 웹하드 서비스, 네이버 TV 같은 비디오 스트리밍 트래픽을 식별할 수 있기 때문에 세분화해서 트래픽을 제어할 수 있다.

NAME	CATEGORY	SUBCATEGORY	RISK	TECHNOLOGY
naver-blog-posting	collaboration	web-posting	2	browser-based
naver-line	collaboration	voip-video	1	client-server
naver-mail	collaboration	email	3	browser-based
naver-ndrive	general-internet	file-sharing	4	browser-based
naver-streaming	media	photo-video	3	browser-based

그림 6. 네이버 트래픽 식별 목록 / 출처 : 팔로알토 네트워스

아래 [그림 7]은 유튜브 트래픽 식별 목록이다. 영상을 시청하는 것 이외에도 영상을 업로드하는 트래픽도 식별할 수 있는 것을 확인할 수 있다.

youtube				
└ youtube-posting	collaboration	web-posting	3	browser-based
└ youtube-tv	media	photo-video	1	browser-based
└ youtube-tv-streaming	media	photo-video	2	browser-based
└ youtube-base	media	photo-video	4	browser-based
└ youtube-safety-mode	media	photo-video	4	browser-based
└ youtube-uploading	media	photo-video	4	browser-based
└ youtube-streaming	media	photo-video	4	browser-based

그림 7. 유튜브 트래픽 식별 목록 / 출처 : 팔로알토 네트워스

다음 [그림 8]은 국민 메신저인 카카오톡 트래픽 식별 목록이다. 만약에 카카오톡 서비스를 모두 차단한다면 회사 임직원들의 원성이 대단할 것이다. 이럴 경우 채팅서비스는 허용하고 파일 전송 기능만 차단하여 보안을 강화하면서 임직원의 민원도 해결할 수 있을 것 같다.

NAME	CATEGORY	SUBCATEGORY	RISK	TECHNOLOGY
kakaomap	general-internet	internet-utility	1	browser-based
kakaotalk				
└ kakaotalk-audio-chat	collaboration	instant-messaging	1	client-server
└ kakaotalk-base	collaboration	instant-messaging	2	client-server
└ kakaotalk-file-transfer	general-internet	file-sharing	2	client-server
kakaotv	media	photo-video	1	browser-based
vakaka	media	photo-video	3	peer-to-peer

그림 8. 카카오톡 트래픽 식별 목록 / 출처 : 팔로알토 네트워스

마지막으로 아래 [그림 9]와 같이 사진 기반으로 운영되는 SNS인 인스타그램도 단순한 검색과 포스팅 트래픽을 구별할 수 있어 좀 더 유연한 보안정책을 설정할 수 있다.

NAME	CATEGORY	SUBCATEGORY	RISK	TECHNOLOGY
cinemagram	media	photo-video	2	client-server
instagram				
└ instagram-base	media	photo-video	2	client-server
└ instagram-upload	media	photo-video	2	client-server

그림 9. 인스타그램 트래픽 식별 목록 / 출처 : 팔로알토 네트워스

지금까지 차세대방화벽의 애플리케이션 탐지 기능에 대해 살펴보았다. 대략 10년 전부터 차세대방화벽이 도입되기 시작하면서, 최근에 도입되는 방화벽은 모두 차세대방화벽을 표방하고 있다. 대부분의 벤더는 애플리케이션 탐지 기능을 기본 기능으로 제공하지 않고 별도의 서비스 라이선스를 구매해야 사용을 허가한다. 그 이유는 새로운 서비스가

계속 등장하고 있어 거기에 맞추어 식별 목록을 계속 업데이트해야 하기 때문이다. 보통 연 단위로 라이선스를 갱신해야 장비에서 업데이트된 식별 목록을 주기적으로 다운로드 받을 수 있다.

다음으로 웹 방화벽에 대해 알아보자. 영어로는 Web Application Firewall이라고 부르며 통상 줄여서 와프(WAF)라고 부른다. 앞에서 설명한 차세대방화벽도 Web 트래픽은 식별할 수 있기에 웹 방화벽과 동일한 기능을 지원하지 않을까 생각할 수 있다. 그러면 여기서 차세대방화벽과 웹 방화벽의 차이점을 먼저 알아보자.

차세대방화벽은 모든 트래픽에 대해 L7 레벨을 모니터링하고 제어할 수 있는 장비이며, 네트워크의 다양한 트래픽을 관리할 수 있는 장비라면, 웹 방화벽은 HTTP, HTTPS 트래픽만 집중해서 모니터링하여 웹서버해킹을 방지하는 목적으로 http method(get, put)와 같은 세부적인 옵션값에 따라 임계치를 설정하여 차단하는 장비로써 차세대방화벽으로 차단이 불가능한 웹 기반 공격을 전문적으로 탐지·차단하는 보안 장비이다. 일반적으로 차세대방화벽이 설치되어 있더라도 업무상 혹은 비즈니스 목적으로 운영되는 웹 기반 서버가 있다면 추가로 웹 방화벽을 설치하여 웹 서버의 보안을 강화하는 것이 일반적인 적용 사례이다.

그럼 웹 방화벽이 등장한 배경을 알아보자. 앞에서 설명한 1세대 혹은 차세대방화벽의 보급이 늘어나면서, 서비스하지 않는 모든 포트는 방화벽의 보안정책으로 차단되게 되었다. 보통 서버들은 OS가 설치되면서 사용하지 않는 포트가 기본적으로 오픈되는 경우가 여러 개 있었다. 예를 들면 윈도우 OS를 설치하면 파일 공유, 원격접속 등을 위한 포트가 기본으로 오픈되면서 방화벽에서 차단되지 않으면, 인터넷을 통해서도 접속이 가능한 경우도 있었다. 이렇게 기본적으로 오픈되는 포트로 인해 많은 공격이 이루어졌지만, 방화벽의 보급이 늘어나고, 서비스하는 포트 이외에는 인터넷을 통해 접근이 불가능해지면서, 공격자의 공격대상이 줄어들게 되었다.

그런데 대부분의 조직에서 웹 서버는 기본적으로 사용하기 때문에 방화벽에서 HTTP, HTTPS 서비스 포트는 열지 않을 수가 없다. 공격자의 입장에서는 HTTP, HTTPS 이외에는 열려 있는 포트가 없다 보니, 웹 서비스만 집중적으로 연구해서 공격 기술을 개발할 수밖에 없는 환경이 된 것이다. 이렇게 웹 기반 공격이 점점 발전되어 다양화되면서, 홈페이지 등이 변조되거나, 웹 서버를 해킹한 후에 이를 통해 사내의 DB 서버에 접근해서 조직의 정보를 탈취하는 일이 빈번하게 발생하였다. 이런 웹 기반의 공격에 대응하기 위해 웹 공격 유행을 분석하여 3~4년 단위로 유행하는 Top 10을 연구하여 발표하는 조직이 있다.

OWASP(Open Web Application Security Project)라는 일종의 커뮤니티로 다양한 개발자, 보안관리자 등이 자발적으로 참여하여 조직한 비영리단체로 OWASP Top 10이란 이름으로 주기적으로 보고서를 발표한다. 최근 발표된 버전은 2017로서 다음 페이지의 [그림 10]과 같이 A1부터 A10까지 가장 빈번하게 발생하는 웹 공격 10개를 나열하고 공격별 취약점 확인 방법과 보안 대책을 설명하고 있다.

제일 빈번하게 발생하는 공격인 인젝션(Injection, 주입)의 경우 말 그대로 클라이언트의 입력값을 조작하여 비정상적인 명령어를 주입하고, 해당 서버의 DB에 있는 다양한 정보를 탈취하거나 관리자 권한을 획득하는 공격 방법이다. 쉬우면서도 공격 성공률이 높은 유형으로 2017년 3월에 발생한 '여기어때'라는 숙박 정보 회사의 고객 DB 정보를 통해 가입자 절반인 99만 명의 이름, 휴대전화번호, 숙박이용정보가 노출되는 사고도 이 공격으로 발생한 사고였다.

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – 인젝션	→	A1:2017 – 인젝션
A2 – 취약한 인증과 세션 관리	→	A2:2017 – 취약한 인증
A3 – 크로스 사이트 스크립팅 (XSS)	↘	A3:2017 – 민감한 데이터 노출
A4 – 안전하지 않은 직접 객체 참조 [A7 항목과 병합됨]	∪	A4:2017 – XML 외부 개체 (XXE) [신규]
A5 – 잘못된 보안 구성	↘	A5:2017 – 취약한 접근 통제 [합침]
A6 – 민감한 데이터 노출	↗	A6:2017 – 잘못된 보안 구성
A7 – 기능 수준의 접근 통제 누락 [A4 항목과 병합됨]	∪	A7:2017 – 크로스 사이트 스크립팅 (XSS)
A8 – 크로스 사이트 요청 변조 (CSRF)	☒	A8:2017 – 안전하지 않은 역직렬화 [신규, 커뮤니티]
A9 – 알려진 취약점이 있는 구성요소 사용	→	A9:2017 – 알려진 취약점이 있는 구성요소 사용
A10 – 검증되지 않은 리다이렉트 및 포워드	☒	A10:2017 – 불충분한 로깅 및 모니터링 [신규, 커뮤니티]

그림 10. OWASP Top 10 2013, 2017 비교

가장 대표적으로 SQL Injection 공격방식은 [그림 11]에 있는 1번과 같이 정상적인 SQL 명령어가 있다고 하자. 여기에 2번과 같이 ' OR 1=1 --'이라는 문구를 중간에 삽입하여 3번과 같이 SQL 명령어를 웹 서버로 전송하게 한다. 1번 명령어는 ID가 INPUT1이고 패스워드가 INPUT2인 사용자의 모든 정보를 불러오게 하는 명령어인데 여기에 특정 문구를 삽입해서 3번과 같이 변조하여 서버로 전송하게 되면, 삽입한 문구 중 '--' 뒤에 있는 문구는 모두 주석 처리되고, OR 1=1은 언제나 True가 되기에 결과적으로 서버에서는 유저테이블에 있는 모든 정보를 불러오게 하는 명령어로 인식되어 서버가 보유한 모든 유저의 정보가 공격자에게 출력되는 결과가 초래하게 된다.

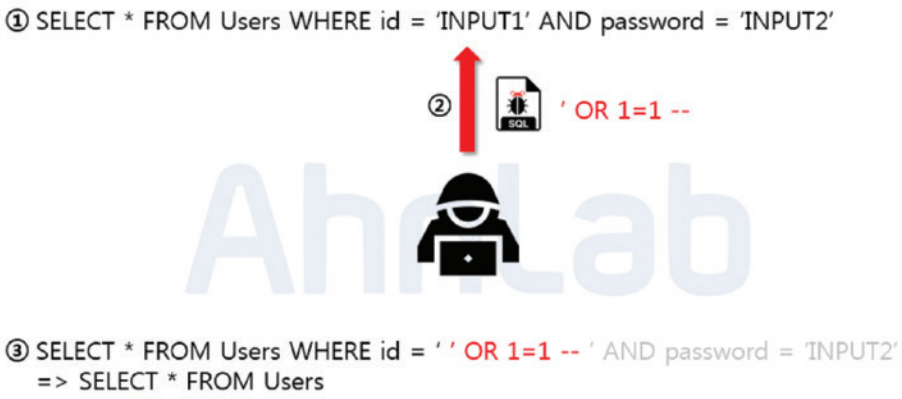

그림 11. SQL Injection 공격방식 / 출처 : 안랩

그러면 이런 공격을 웹 방화벽에서는 어떻게 차단할 수 있는지 알아보자. 웹 방화벽은 웹 서버 앞에서 사전에 HTTP 패킷을 분석하여 정상적이라고 판단되는 트래픽만 웹 서버로 전달한다. [그림 12]와 같이 트래픽이 들어오면 아래와 같은 여러 가지 단계의 분석을 통해 공격을 차단한다.

1. 패킷의 L7 레벨을 확인하여 정상적인 HTTP 구문인지 먼저 확인한다.
2. URI(예 : www.abc.com/user)를 식별하여 적용되는 정책을 확인하고 어떤 공격 탐지 rule을 적용하여 검사할 것인지 판단한다.

3. 적용된 공격 탐지 룰에 따라 여러 가지 공격을 탐지한다. 이때 블랙리스트(black list)를 이용하여 사용할 수 없는 구문이나 패턴을 먼저 차단한다.
4. 화이트리스트(white list)를 이용하여 허용된 구문 또는 패턴을 통과시킨다.
5. 정상적인 시도라도 임계치 설정을 통해 짧은 시간 동안 여러 번의 시도가 있으면 차단한다.
6. 서버에서 응답하는 웹 페이지가 변조되어 있는지, 에러 코드를 반환을 통해 공격자에게 정보를 제공하는지 확인하여, 관리자에게 경보를 알리거나 반환 값을 숨긴다.

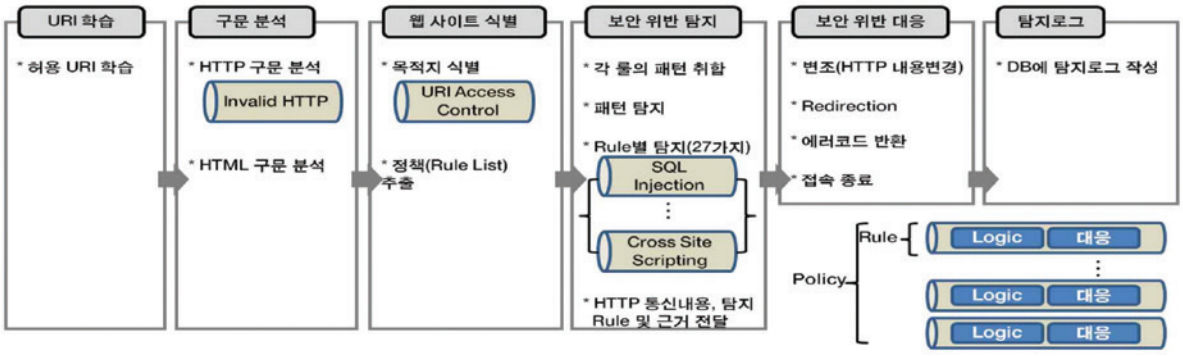

그림 12. 웹 방화벽의 공격 트래픽 분석 프로세스 / 출처 : 펜타시큐리티

웹 방화벽의 경우도 일반 방화벽과 같이 시간이 지나면서 점점 발전을 거듭하였다. 초기 웹 방화벽은 사전에 관리자가 설정하는 화이트리스트, 블랙리스트에 의존하기 때문에 오탐(정상적인 트래픽인데 공격으로 판단하는 경우), 미탐(공격 트래픽인데 탐지하지 못하는 경우)이 발생하는 경우가 매우 빈번하였다. 이런 문제는 웹 방화벽이 URI(예 : www.daum.net/news), 웹 트래픽 내용을 모니터링하여 학습하면서 정상적인 접속 내용은 화이트리스트를 자동으로 추가하거나, 기존에 학습된 내용과 현저히 다른 내용이 보이면 공격으로 판단하는 등 사전에 등록된 패턴에 의존하지 않고, 유사도 등을 측정하여 공격을 차단하는 방식이 사용되었다.

최근에는 정치적이거나 민족주의적인 이유, 예를 들면 815 광복절에 일본 해커가 독도 홍보사이트를 공격하여 홈페이지 내용의 위변조를 시도하는 것 같이 과시형 공격이나, 웹 서버를 통해 고객 자료를 탈취하여 비트코인 등의 금품을 요구하는 행위 등 다양한 공격이 웹 서버를 대상으로 이루어지고 있다. 쇼핑몰, 서비스 예약, 웹 포탈, 홍보사이트와 같이 조직의 비즈니스가 웹에서 대부분 이루어지는 조직에서 이제 웹 방화벽이 필수적인 보안 장비가 되었다.

다음 호에서는 클라우드에 활용되는 가상화 기술이 발전하면서 보안 장비에 어떻게 가상화 기술이 적용되는지 소개하도록 하겠다.